(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年10月13日(13.10.2005)

PCT

(10) 国际公布号:
WO 2005/096644 A1

(51) 国际分类号[7]: H04Q 7/24

(21) 国际申请号: PCT/CN2005/000376

(22) 国际申请日: 2005年3月24日(24.03.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200410030517.1 2004年4月2日(02.04.2004) CN

(71) 申请人(对除美国以外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 黄迎新(HUANG, Yingxin) [CN/CN]; 张文林(ZHANG, Wenlin) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW COPRORATION); 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

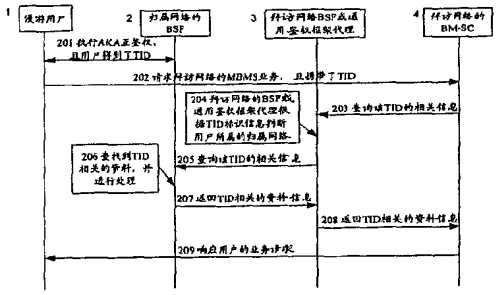
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ,

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A METHOD FOR ESTABLISHING SECURITY ASSOCIATION BETWEEN THE ROAMING SUBSCRIBER AND THE SERVER OF THE VISITED NETWORK

(54) 发明名称: 漫游用户与拜访网络内的业务服务器建立信任关系的方法



(57) Abstract: A method for establishing security association between the roaming subscriber and the server of the visited network, and after receiving the service request from a roaming. subscriber, the server of the visited network establishes security association with the roaming subscriber by the BSF or the general authentication frame agent or the AAA server of this network and the AAA server of the home network of the roaming subscriber according to the authenticating result of the general authentication frame in the home network; it is achieved that the roaming subscriber employs the service of its visited network after being authenticated through the general authentication frame of the home network.

[见续页]

WO 2005/096644 A1

(57) 摘要

本发明提供了一种漫游用户与拜访网络内业务服务器建立信任关系的方法，当拜访网络中的业务服务器接收到来自漫游用户的业务请求后，通过本网络的BSF，或本网络的通用鉴权框架代理，或本网络内的AAA服务器以及该漫游用户所属归属网络内的AAA服务器，利用归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务服务器和漫游用户之间的信任关系；从而实现了漫游用户经过归属网络内的通用鉴权框架鉴权后使用其所在拜访网络内的业务。

漫游用户与拜访网络内的业务服务器建立信任关系的方法

技术领域

本发明涉及第三代无线通信技术领域，特别是指一种漫游用户与拜访网络内的业务服务器建立信任关系的方法。

发明背景

在第三代无线通信标准中，通用鉴权框架是多种应用业务实体使用的一个用于完成对用户身份进行验证的通用结构，应用通用鉴权框架可实现对应用业务的用户进行检查和验证身份。上述多种应用业务可以是多播/广播业务、用户证书业务、信息即时提供业务等，也可以是代理业务。

图 1 所示为通用鉴权框架的结构示意图。通用鉴权框架通常由用户终端（UE）101、执行用户身份初始检查验证的实体（BSF）102、用户归属网络服务器（HSS）103 和网络应用实体（NAF）104 组成。BSF 102 用于与用户终端 101 进行身份互验证，同时生成 BSF 102 与用户 101 的共享密钥；HSS 103 中存储有用于描述用户信息的描述（Profile）文件，该 Profile 中包括用户身份标识等所有与用户有关的描述信息，同时 HSS 103 还兼有产生鉴权矢量信息的功能。

用户需要使用某种业务时，如果其知道需要首先与 BSF 进行互鉴权过程，则直接与 BSF 联系进行互鉴权，否则，用户会首先和该业务对应的 NAF 联系，如果该 NAF 使用通用鉴权框架，并且发现发出请求的用户还未与 BSF 进行互鉴权，则通知发出请求的用户与 BSF 进行互鉴权以验证身份。

用户与 BSF 之间的互认证过程是：BSF 接到来自用户的鉴权请求后，

首先到 HSS 获取该用户的鉴权信息，根据所获取的鉴权信息与用户之间执行鉴权和密钥协商协议（AKA）进行互鉴权。认证成功后，用户和 BSF 之间互相认证了身份并且同时生成了共享密钥 Ks。之后，BSF 分配一个会话事务标识（B-TID）给用户，该 B-TID 是与 Ks 相关联的。

用户收到这个 B-TID 后，重新向 NAF 发出连接请求，且请求中携带了该 B-TID。接收到请求的 NAF 确认该用户合法且获得了共享密钥 Ks 或由 Ks 衍生的密钥后，该用户应用 B-TID 与 NAF 在密钥 Ks 或 Ks 衍生密钥的保护下进行正常的通信。

下面以多播/广播业务（MBMS）为例，具体说明通用鉴权框架的用法。在无线通信领域中，多播业务是一种一点到多点的单向承载业务，数据是由一个源实体，传送到多个接收实体。在某一区域内已订阅多播业务的用户，能够接收多播业务的服务。在多播业务中需要防止没有订阅或未付费的用户享受多播业务，因此在多播业务的群组中，针对某个具体业务都设置有一个多播服务密钥（MSK），MSK 只有群组内的用户和提供多播业务的服务器知道，而群组外的用户无权知道这个密钥。共享的 MSK 并不直接加密 MBMS 业务数据，只用来做接入控制，产生多播业务密钥（MTK），且 MSK 对 MTK 进行加密。多播业务服务器使用 MTK 对业务数据信息进行加密，群组内的用户收到业务数据信息后使用相同的共享 MTK 解密，从而获得业务数据信息的内容，而群组外用户因为没有这个共享密钥，所以不能获取多播信息内容。

用户应用 MBMS 时，首先要经过通用鉴权框架的鉴权，即应用通用鉴权框架中的 BSF 代替 MBMS 的服务器对用户进行鉴权，而 MBMS 中的多播/广播服务器（BM-SC）则相当于通用鉴权框架中的 NAF。BSF 对用户进行鉴权后，BSF 与用户共享了密钥 Ks，并且 BSF 给该用户分配了 B-TID，然后用户使用 B-TID 向 BM-SC 发出业务请求，BM-SC 收

到用户包含 B-TID 的请求后，向 BSF 进行查询，BSF 查到该用户的信息后，返回密钥 Ks 或 Ks 衍生的密钥。这样 BM-SC 与用户也就共享了密钥 Ks 或由 Ks 衍生的密钥，该共享密钥即为 MBMS 业务中的多播用户密钥（MUK），用来保护 BM-SC 到用户之间点到点的群组共享密钥 MSK。也就是说，此时，用户与 BM-SC 之间建立了信任关系（security association），即用户相信它所连接的服务器是真实而且合法的服务器，而不是由其它设备假冒的服务器，同时业务服务器也相信请求业务的用户是一个合法用户，而不是一个攻击者。该信任的基础就是所拥有的相同共享密钥 MUK，在后面的通信过程中，通过该共享密钥 MUK 来确认对方确实是对方。

上述基于通用鉴权框架的应用方式，仅限于用户在其归属网络内使用。也就是说，在现有技术中，只考虑了用户在其归属网络中使用通用鉴权框架问题，没有考虑用户在漫游状态下使用拜访网络业务时，如何使用其归属网络内的通用鉴权框架的问题。

在实际应用中，已应用通用鉴权框架通过鉴权的用户处于漫游状态时，通常需要使用拜访网络的某些业务，例如漫游用户需要了解当地新闻、天气、交通等信息。由于现有技术没有考虑在拜访网络中如何使用归属网络的通用鉴权框架，因此将导致漫游的用户不能应用通用鉴权框架与拜访网络的业务服务器建立信任关系，从而使得已经通过通用鉴权框架鉴权的漫游用户不能使用拜访网络中的业务。

发明内容

有鉴于此，本发明的目的在于提供一种漫游用户与拜访网络内的业务服务器建立信任关系的方法，使漫游用户和拜访网络的业务服务器能够通过该用户所属归属网络内的通用鉴权框架建立信任关系。

为达到上述目的，本发明的技术方案是这样实现的：

一种漫游用户与拜访网络内业务服务器建立信任关系的方法，漫游用户已与其所属归属网络内的通用鉴权框架中的执行用户身份初始检查验证实体BSF完成互鉴权，获得BSF为其分配的会话事务标识B-TID，该方法包括以下步骤：

拜访网络内的业务服务器接收到来自漫游用户的包含B-TID的业务请求消息后，利用该漫游用户所属归属网络的通用鉴权框架对该漫游用户进行鉴权的鉴权结果，获取该漫游用户的用户信息，建立起与漫游用户之间信任关系。

较佳地，所述获取漫游用户的用户信息的过程包括以下步骤：

a、拜访网络内的业务服务器向本网络内的 鉴权实体发送查询该B-TID 所对应的用户信息的消息；

b、接收到步骤 a 所述查询消息的鉴权实体根据消息中的 B-TID 确定漫游用户所属的归属网络；从该漫游用户所属的归属网络的 BSF 中获取该B-TID对应的用户信息，并将所获取的用户信 息返回给业务服务器；

c、拜访网络内的业务服务器根据鉴权实体返回的消息获取用户信息。

较佳地，所述拜访网络内的鉴权实体为拜访网络内的 BSF 或通用鉴权框架代理；

所述拜访网络内的 BSF 或通用鉴权框架代理从该漫游用户所属的归属网络的 BSF 中获取该 B-TID 对应的用户信息 的方法为：

拜访网络内的 BSF 或通用鉴权框架代理直接向该漫游用户所属归属网络内的 BSF 发送查询与该 B-TID 所对应的用 户信息的消息；从该漫游用户所属归属网络内的BSF返回的响应消息中获取该B-TID对应的用户信息。

较佳地，所述拜访网络内的通用鉴权框架代理是一个独立的服务器，或与本网络内的 AAA 服务器合设的服务器，或与本网络内的业务服务器合设的服务器。

较佳地，所述拜访网络内的鉴权实体为拜访网络内的 AAA 服务器；

所述拜访网络内 AAA 服务器从该漫游用户所属的归属网络的 BSF 中获取与该 B-TID 对应的用户信息的方法为：

拜访网络内 AAA 服务器向该漫游用户所属的归属网络的 AAA 服务器发送查询与该 B-TID 所对应的用户信息的消息；

归属网络内的 AAA 服务器直接向本网络中的 BSF 进行查询，BSF 在本地查询到与该 B-TID 对应的用户信息后，给本网络中的 AAA 服务器返回包含与该 B-TID 对应的用户信息的响应消息，由本网络中 的 AAA 服务器给拜访网络中的 AAA 服务器返回包含与该 B-TID 对应的用户信息的响应消息；拜访网络中的 AAA 服务器从该漫游用户所属归属网络内的 AAA 服务器返回的响应消息中获取该 B-TID 对应的用户信息。

较佳地，如果拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络不识别 B-TID，则所述获取漫游用户的用户信息的过程包括以下步骤：

a、拜访网络内的业务服务器通知漫游用户 TI 为非法标识， 并提示用户使用永久身份标识；

b、拜访网络内的业务服务器再次接收到来自漫游用户的包含永久身份标识的业务请求信息后，向本网络内的 AAA 服务器发出鉴权请求；拜访网络内的 AAA 服务器根据用户的永久身份标识确认该用户所属的归属网络，向该漫游用户所属归属网络内的 AAA 服务器发送对该用户进行鉴权的请求；

c、归属网络内的 AAA 服务器接收到来自拜访网络 AAA 服务器的

鉴权请求后，请求本网络内的 BSF 对该用户进行鉴权;

d、归属网络内的 BSF，经本网络内的 AAA 服务器、拜访网络内的 AAA 服务器以及拜访网络内的业务服务器，与该用户进行互鉴权，鉴权成功后，直接给本网络内的 AAA 服务器返回鉴权成功消息，由本网络中的 AAA 服务器给拜访网络中的 AAA 服务器返回鉴权成功消息; 所述授权消息中包含有用户信息;

e、拜访网络内的业务服务器根据本网络内的 AAA 服务器返回的鉴权成功消息中获取该漫游用户的用户信息。

较佳地，所述用户信息中至少包括：密钥信息和用户的身份标识。

较佳地，所述用户信息中还包括与安全相关的描述 profile 信息。

较佳地，所述密钥信息是鉴权时产生的共享密钥 Ks，或共享密钥 Ks 的衍生密钥及该衍生密钥的有效期限。

应用本发明，当拜访网络内的业务服务器接收到来自漫游用户的包含 B-TID 信息的业务请求消息后，根据该漫游用户所属归属网络的通用鉴权框架鉴权结果，建立拜访网络业务服务器和漫游用户之间的信任关系，从而实现了漫游用户通过该用户所属归属网络内的通用鉴权框架使用拜访网络内的业务。由于本发明使得漫游用户在使用拜访网络业务时，仍然可以使用本网通用鉴权框架的鉴权结果，因而充分利用了现有网络结构，节省了资源。本发明增加了一种用户使用拜访网络业务的途径，使得拜访网络能够最大限度的为用户提供业务。另外，即使拜访网络内的业务服务器完全不认识 B-TID 标识，漫游用户也可以应用其所属网络的通用鉴权框架完成鉴权过程，从而减少了由 AAA 服务器进行鉴权时因序列号（SQN）失步造成的鉴权失败的情况。

附图简要说明

图 1 所示为通用鉴权框架的结构示意图;

图 2 所示为应用本发明实施例一的示意图;

图 3 所示为应用本发明实施例二的示意图;

图 4 所示为应用本发明实施例三的示意图。

实施本发明的方式

为使本发明的技术方案更加清楚，下面结合附图及具体实施例再对本发明做进一步地详细说明。

本发明的思路是：拜访网络中的业务服务器接收到来自漫游用户的业务请求后，通过本网络的 BSF，或本网络的通用鉴权框架代理，或本网络内的 AAA 服务器以及该漫游用户所属归属网络内的 AAA 服务器，利用归属网络的通用鉴权框架的鉴权结果，获取用户信息，从而建立拜访网络业务服务器和漫游用户之间的信任关系；使得漫游用户经过归属网络内的通用鉴权框架鉴权后可以使用其所在拜访网络内的业务。

为了更好地说明漫游用户如何通过归属网络中的通用鉴权框架与拜访网络内的业务服务器建立信任关系，下面首先说明几种可能存在的情况。

对于漫游用户而言，其可能需要使用归属网络中的业务，也可能需要使用拜访网络中的业务。

当漫游用户使用归属网络中的业务时，由于网络间都是 IP 连接，因而漫游用户可通过应用层直接与归属网络中的业务服务器进行通信，并可以直接使用归属网络中的通用鉴权框架。这与现有的使用方法完全相同。

下面具体说明漫游用户使用拜访网络内业务的情况。

对于漫游用户所在的拜访网络而言，其可能存在以下四种情况：

1）该用户所在的拜访网络支持通用鉴权框架。

2）该用户所在的拜访网络不支持通用鉴权框架，但支持通用鉴权框架代理。在这种情况下，拜访网络内可能存在一个单独的支持通用鉴权框架代理的服务器，但在实际应用中，通常会将该服务器与其它实体合设，例如将支持通用鉴权框架代理的服务器与 AAA 合设，由 AAA 实现支持通用鉴权框架代理的功能，即由 AAA 实现对 B-TID 分析和路由功能；拜访网络内也可能不存在支持通用鉴权框架代理的单独的服务器，而是拜访网络中的各个服务器均支持通用鉴权框架代理功能，即由每个实际的业务服务器实现对 B-TID 分析和路由功能。由于 1）和 2）的处理方法很类似，在下面以一个实施例加以说明。

3）该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器不对 B-TID 进行鉴别，也不对 B-TID 进行处理，仅把 B-TID 看作是一种用户身份标识，并将该标识直接传递给本网络中的 AAA 服务器，请求 AAA 服务器进行鉴权。

4）该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器对自身接收到的标识进行鉴别，但由于在拜访网络中根本没有通用鉴权框架的概念，所以业务服务器不认识 B-TID 标识，因此它要求用户使用自己的永久身份标识，如国际移动用户识别码（IMSI）等。

下面以漫游用户应用其所在拜访网络中的 MBMS 业务为例，具体说明建立信任关系的方法，其中 BM-SC 为 MBMS 业务的业务服务器。

图 2 所示为应用本发明实施例一的示意图。业务服务器通过直接查询该漫游用户在所属归属网络的通用鉴权框架鉴权结果，与漫游用户之间建立信任关系的步骤如下：

步骤 201，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA 互鉴权，鉴权通过后，得到了 BSF 分配的 B-TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks;

步骤 202，漫游用户向拜访网络的 BM-SC 发送包含 B-TID 的业务请求消息;

步骤 203，如果拜访网络支持通用鉴权框架，则 BM-SC 向本网络内的 BSF 发送查询与该 B-TID 相对应的用户信息;

如果拜访网络仅支持通用鉴权框架代理功能，且支持通用鉴权框架代理功能由一个单独的服务器实现，该则 BM-SC 向本网络内实现通用鉴权框架代理的服务器发送查询与该 B-TID 对应的用户信息;

如果拜访网络仅支持通用鉴权框架代理，且支持通用鉴权框架代理功能由每个业务服务器自己实现，则 BM-SC 同样查询与该 B-TID 对应的用户信息，只是该查询是在该业务服务器的内部接口中实现;

步骤 204，拜访网络内的 BSF 或通用鉴权框架代理，根据接收到的 B-TID 确认该漫游用户所属的归属网络;

步骤 205，拜访网络内的 BSF 或通用鉴权框架代理向漫游用户所属归属网络内的 BSF 查询与该 B-TID 对应的用户信息;

步骤 206，归属网络的 BSF 检索到与该 B-TID 对应的用户信息后，根据本地运营商的策略进行处理，即根据运营商的策略决定是将与 B-TID 对应的密钥 Ks 作为用户信息中的密钥信息返回给请求者，还是将密钥 Ks 的衍生密钥，以及该衍生密钥的有效期限作为用户信息中的密钥信息返回给请求者，如果是后者，则进行密钥衍生操作及设定该衍生密钥有效期限的操作;

步骤 207，归属网络的 BSF 给拜访网络的 BSF 或通用鉴权框架代理返回包含该 B-TID 对应的用户信息的响应消息; 上述与该 B-TID 对应的

用户信息包括密钥信息、用户的身份标识，和与安全相关的 profile 信息，其中，密钥信息和用户的身份标识是必选项，密钥信息用于保证用户与 BM-SC 之间进行正常的通信，用户的身份标识用于计费，如果拜访网络不能确定用户的真实身份，在其与归属网络进行网间结算时将出现问题；与安全相关的 profile 信息是可选项；

步骤 208，拜访网络的 BSF 或通用鉴权框架代理将 B-TID 的相关信息返回给 BM-SC，BM-SC 收到与该 B-TID 对应的用户信息后，也就和 UE 共享了 Ks 或由 Ks 衍生的密钥，该密钥作为 MBMS 业务的 MUK，用于保护群组共享密钥 MSK 的点到点保密传送；

此时 BM-SC 也就与该漫游用户建立了信任关系，认为该发起请求的漫游用户合法。这是因为，如果 BM-SC 能够查询到与该 B-TID 对应的用户信息，则说明该用户已经通过了鉴权，该用户是一个合法的用户，并且和该漫游用户之间有了共享密钥，在后面的通信过程中，通过该共享密钥来相互确认对方；反之，如果 BM-SC 不能够查询到与该 B-TID 对应的用户信息，则说明该用户还没有通过鉴权，该用户目前还是一个非法的用户。

步骤 209，BM-SC 发确认消息给该用户，并和该用户进行 MBMS 业务内部密钥分发，业务发送等相关的业务过程。

至此，漫游用户实现了利用归属网络中的通用鉴权框架使用拜访网络中的业务。上述方法适用于漫游用户所在拜访网络支持通用鉴权框架，或支持通用鉴权框架代理的情况。

图 3 所示为应用本发明实施例二的示意图。业务服务器通过直接查询该漫游用户在所属归属网络的通用鉴权框架鉴权结果，与漫游用户之间建立信任关系的步骤如下：

步骤 301，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA

互鉴权，鉴权通过后，得到了 BSF 分配的 B-TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks;

步骤 302，漫游用户向拜访网络的 BM-SC 发送包含 B-TID 信息的业务请求消息;

步骤 303，拜访网络的 BM-SC 不检查该用户的身份是否合法，而是直接将该 B-TID 作为用户身份标识，向本网络内的 AAA 服务器发出查询请求，即请求本网络的 AAA 对该用户进行鉴权，即判断该用户是否合法;

步骤 304，拜访网络的 AAA 服务器根据 B-TID 标识的格式（B-TID 的标识格式为用户标识@域名），判断出用户所属的归属网络;

步骤 305，拜访网络的 AAA 服务器向该漫游用户所属归属网络内的 AAA 服务器发出查询 B-TID 的请求，即请求归属网络内的 AAA 服务器对该用户进行鉴权;

步骤 306，归属网络内的 AAA 服务器收到查询 B-TID 的消息后，由于其知道 B-TID 标识是由本网的通用鉴权框架中的 BSF 分配的，因此其向 BSF 进行查询；BSF 和 AAA 服务器在某些执行功能上是类似的，所以 BSF 也可能是由网络中的某个 AAA 服务器来兼任，在这种情况下，BSF 和 AAA 服务器之间的消息是内部接口消息;

步骤 307，归属网络的 BSF 检索到与该 B-TID 对应的用户信息后，根据本地运营商的策略进行处理，即根据运营商的策略决定是将与 B-TID 对应的密钥 Ks 作为用户信息中的密钥信息返回给请求者，还是将密钥 Ks 的衍生密钥，以及该衍生密钥的有效期限作为用户信息中的密钥信息返回给请求者，如果是后者，则进行密钥衍生操作及设定该衍生密钥有效期限的操作;

步骤 308，归属网络的 BSF 给本网络的 AAA 服务器返回包含该

B-TID 对应的用户信息的响应消息；上述与该 B-TID 对应的用户信息包括密钥信息、用户的身份标识，和与安全相关的 profile 信息，其中，密钥信息和用户的身份标识是必选项，密钥信息用于保证用户与 BM-SC 之间进行正常的通信，用户的身份标识用于计费，如果拜访网络不能确定用户的真实身份，在其与归属网络进行网间结算时将出现问题；安全相关的 profile 信息是可选项；

步骤 309，归属网络的 AAA 服务器给拜访网络内的 AAA 服务器返回包含与该 B-TID 对应的用户信息的响应消息；拜访网络内的 AAA 服务器接收到归属网络的 AAA 服务器返回的消息后，即认为归属网络已经对用户进行了鉴权，该查询返回消息相当于授权消息；

步骤 310，拜访网络的 AAA 服务器给 BM-SC 返回包含与该 B-TID 对应的用户信息的响应消息，BM-SC 从接收到的响应消息中获取该 B-TID 对应的用户信息，同时，BM-SC 也和 UE 共享了 Ks 或由 Ks 衍生的密钥，该密钥作为 MBMS 业务的 MUK，用于保护群组共享密钥 MSK 的点到点保密传送；即只要 BM-SC 获取了漫游用户的用户信息，BM-SC 就建立起了与漫游用户之间的信任关系，认为该发起请求的漫游用户合法；

步骤 311，BM-SC 发确认消息给该用户，并和该用户进行 MBMS 业务内部密钥分发，业务发送等相关的业务过程。

至此，漫游用户实现了利用归属网络中的通用鉴权框架使用拜访网络中的业务。上述方法适用于漫游用户所在拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器不鉴别 B-TID 标识，只是将其作为一种用户身份标识，传递给本网络中的 AAA 服务器，请求 AAA 服务器对该用户进行鉴权的情况。

在上述两个实施例中，BM-SC 是向本网络内的 BSF 或通用鉴权框

架代理，或者向本网络内的 AAA 服务器发送查询用户信息的消息，推而广之，本领域技术人员可以很容易想到，BM-SC 还可以依照上述方法向网络中的其他鉴权实体发送查询用户信息的消息，在此，并不对具体的鉴权实体加以限制。

图 4 所示为应用本发明实施例三的示意图。业务服务器通过与该漫游用户所属归属网络的通用鉴权框架实施鉴权过程，获取鉴权结果，根据该鉴权结果与漫游用户之间建立信任关系的步骤如下：

步骤 401，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA 互鉴权，鉴权通过后，得到了 BSF 分配的 B-TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks;

步骤 402，漫游用户向拜访网络的 BM-SC 发送包含 B-TID 信息的业务请求消息;

步骤 403，由于 BM-SC 不能识别 B-TID 标识，因此 BM-SC 通知漫游用户该标识非法，并提示用户使用永久身份标识，如 IMSI 等;

步骤 404，漫游用户向 BM-SC 发送包含永久身份标识的业务请求;

步骤 405，拜访网络的 BM-SC 向本网络内的 AAA 服务器发出鉴权请求;

步骤 406，拜访网络的 AAA 服务器根据用户的身份标识判断出该漫游用户所属的归属网络，然后向该漫游用户所属归属网络内的 AAA 服务器发出鉴权请求;

步骤 407，归属网络内的 AAA 服务器请求本网络内的通用鉴权框架中的 BSF 进行鉴权，这是因为：虽然 AAA 服务器本身具有鉴权计费功能，且在地位上是与 BSF 相同的，但在实际应用中，不同的 AAA 服务器在对用户进行鉴权时，容易出现因序列号（SQN）失步而导致鉴权失败的情况，出现的具体原因在现有已公布的文章中有描述，所以对通用

鉴权框架支持的业务采用通用鉴权框架对用户进行鉴权，以保证鉴权的成功率；

步骤 408，归属网络内 BSF 与用户完成 AKA 的鉴权过程，该鉴权过程中的消息在逻辑上是经过拜访网络的 BM-SC，拜访网络的 AAA，归属网络的 AAA 转发的；

步骤 409，鉴权成功后，归属网络内的 BSF 给拜访网络的 BM-SC 返回鉴权成功消息，该消息中包含鉴权成功及授权信息；因为归属网络内的 BSF 已经知道鉴权请求是来自哪个具体的业务服务器，因此，归属网络内的 BSF 直接将该漫游用户的用户信息包含在该鉴权成功消息中，如果归属网络内的 BSF 在鉴权的同时给用户分配了 B-TID，则该 B-TID 也可以包含在鉴权成功消息中通知 BM-SC 服务器；

步骤 410，归属网络内的 AAA 服务器向拜访网络内的 AAA 服务器转发该鉴权成功消息；该消息中包含有鉴权成功及授权信息，同时还包含有该漫游用户的用户信息；所述用户信息包括密钥信息、用户的身份标识，和与安全相关的 profile 信息，其中，密钥信息和用户的身份标识是必选项，密钥信息用于保证用户与 BM-SC 之间进行正常的通信，用户的身份标识用于计费，如果拜访网络不能确定用户的真实身份，在其与归属网络进行网间结算时将出现问题；安全相关的 profile 信息是可选项；

步骤 411，拜访网络的 AAA 服务器转发鉴权成功消息给 BM-SC，BM-SC 从接收到的消息中获取该漫游用户的用户信息，同时，BM-SC 也和 UE 共享了 Ks 或由 Ks 衍生的密钥，该密钥作为 MBMS 业务的 MUK，用于保护群组共享密钥 MSK 的点到点保密传送；即只要 BM-SC 获取了漫游用户的用户信息，BM-SC 就建立起了与漫游用户之间的信任关系；

如果该鉴权成功消息中包含有 B-TID，而虽然 BM-SC 不能够识别 B-TID，但它仍然可以在后面的通信中使用 B-TID，这时该 B-TID 将作为一种临时身份标识使用，其使用的方法与现有临时身份标识的使用方法相同；

步骤 412，BM-SC 收到鉴权成功消息后，发确认消息给该用户，并和该用户进行 MBMS 业务内部密钥分发，业务发送等相关的业务过程。至于 BM-SC 和用户在后续的通信过程中使用哪种用户身份标识，根据拜访网络运营商的策略而定。

至此，漫游用户实现了利用归属网络中的通用鉴权框架使用拜访网络中的业务。上述方法适用于该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器对用户请求消息中的标识进行鉴别，但因为在拜访网络中根本没有通用鉴权框架的概念，所以业务服务器不能识别 B-TID 标识，因此业务服务器要求用户使用自己的永久身份标识。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种漫游用户与拜访网络内业务服务器建立信任关系的方法，漫游用户已与其所属归属网络内的通用鉴权框架中的执行用户身份初始检查验证实体 BSF 完成互鉴权，获得 BSF 为其分配的会话事务标识 B-TID，其特征在于，该方法包括以下步骤：

拜访网络内的业务服务器接收到来自漫游用户的包含B-TID的业务请求消息后，利用该漫游用户所属归属网络的通用鉴权框架对该漫游用户进行鉴权的鉴权结果，获取该漫游用户的用户信息，建立起与漫游用户之间信任关系。

2、根据权利要求 1 所述的方法，其特征在于，所述获取漫游用户的用户信息的过程包括以下步骤：

a、拜访网络内的业务服务器向本网络内的鉴权实体发送查询该 B-TID 所对应的用户信息的消息；

b、接收到步骤 a 所述查询消息的鉴权实体根据消息中的 B-TID 确定漫游用户所属的归属网络；从该漫游用户所属的归属网络的 BSF 中获取该B-TID对应的用户信息，并将所获取的用户信息返回给业务服务器；

c、拜访网络内的业务服务器根据鉴权实体返回的消息获取用户信息。

3、根据权利要求 2 所述的方法，其特征在于，所述拜访网络内的鉴权实体为拜访网络内的 BSF 或通用鉴权框架代理；

所述拜访网络内的 BSF 或通用鉴权框架代理从该漫游用户所属的归属网络的 BSF 中获取该 B-TID 对应的用户信息的方法为：

拜访网络内的 BSF 或通用鉴权框架代理直接向该漫游用户所属归属网络内的 BSF 发送查询与该 B-TID 所对应的用户信息的消息；从该漫

游用户所属归属网络内的BSF返回的响应消息中获取该B-TID对应的用户信息。

4、根据权利要求 3 所述的方法，其特征在于，所述拜访网络内的通用鉴权框架代理是一个独立的服务器，或与本网络内的 AAA 服务器合设的服务器，或与本网络内的业务服务器合设的服务器。

5、根据权利要求 2 所述的方法，其特征在于，所述拜访网络内的鉴权实体为拜访网络内的 AAA 服务器;

所述拜访网络内 AAA 服务器从该漫游用户所属的归属网络的 BSF 中获取与该 B-TID 对应的用户信息的方法为:

拜访网络内AAA服务器向该漫游用户所属的归属网络的AAA服务器发送查询与该 B-TID 所对应的用户信息的消息;

归属网络内的 AAA 服务器直接向本网络中的 BSF 进行查询，BSF 在本地查询到与该 B-TID 对应的用户信息后，给本网络中的 AAA 服务器返回包含与该B-TID对应的用户信息的响应消息，由本网络中的 AAA 服务器给拜访网络中的 AAA 服务器返回包含与该 B-TID 对应的用户信息的响应消息；拜访网络中的 AAA 服务器从该漫游用户所属归属网络内的 AAA 服务器返回的响应消息中获取该 B-TID 对应的用户信息。

6、根据权利要求 1 所述的方法，其特征在于，所述获取漫游用户的用户信息的过程包括以下步骤:

a、拜访网络内的业务服务器通知漫游用户 B-TID 为非法标识，并提示用户使用永久身份标识;

b、拜访网络内的业务服务器再次接收到来自漫游用户的包含永久身份标识的业务请求信息后，向本网络内的 AAA 服务器发出鉴权请求;拜访网络内的 AAA 服务器根据用户的永久身份标识确认该用户所属的归属网络，向该漫游用户所属归属网络内的 AAA 服务器发送对该用户

进行鉴权的请求;

c、归属网络内的 AAA 服务器接收到来自拜访网络 AAA 服务器的鉴权请求后，请求本网络内的 BSF 对该用户进行鉴权;

d、归属网络内的 BSF，经本网络内的 AAA 服务器、拜访网络内的 AAA 服务器以及拜访网络内的业务服务器，与该用户进行互鉴权，鉴权成功后，直接给本网络内的 AAA 服务器返回鉴权成功消息，由本网络中的 AAA 服务器给拜访网络中的 AAA 服务器返回鉴权成功消息; 所述授权消息中包含有用户信息;

e、拜访网络内的业务服务器根据本网络内的 AAA 服务器返回的鉴权成功消息中获取该漫游用户的用户信息。

7、根据权利要求 1、2、或 6 所述的方法，其特征在于，所述用户信息中至少包括: 密钥信息和用户的身份标识。

8、根据权利要求 7 所述的方法，其特征在于，所述用户信息中还包括与安全相关的描述 profile 信息。

9、根据权利要求 7 所述的方法，其特征在于，所述密钥信息是鉴权时产生的共享密钥 Ks，或共享密钥 Ks 的衍生密钥及该衍生密钥的有效期限。

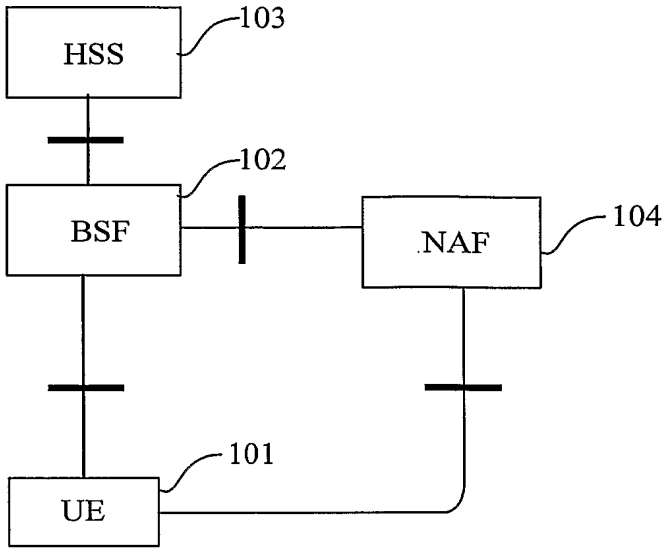

HSS
103
BSF
102
NAF
104
UE
101

图 1

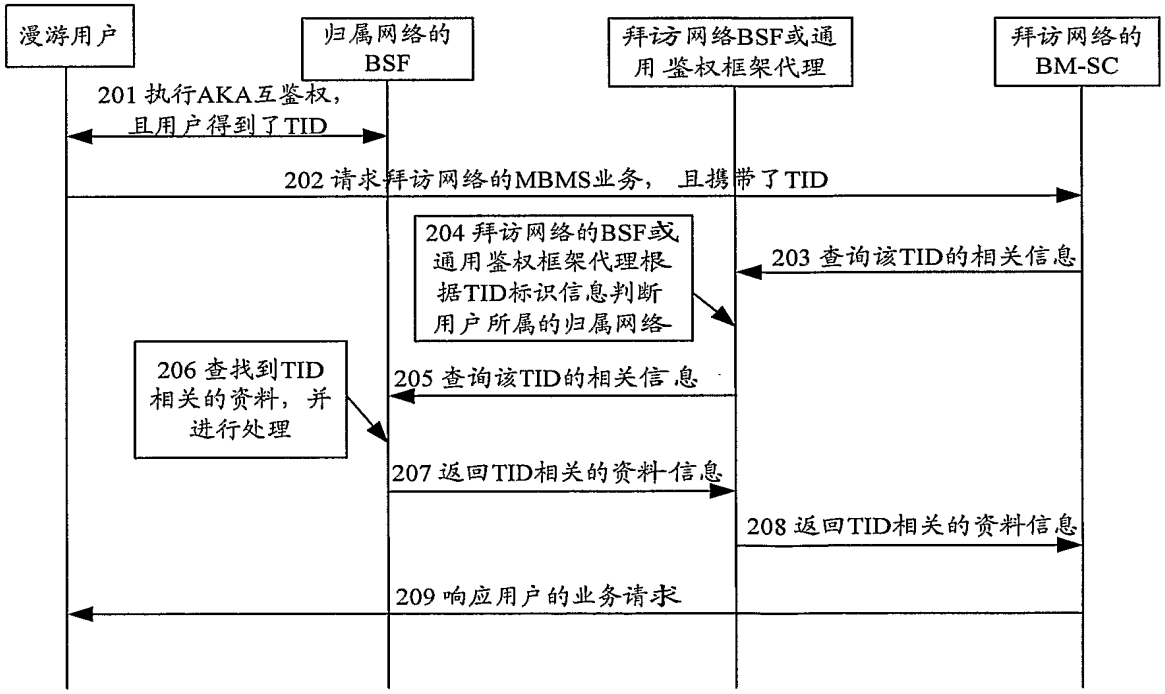

漫游用户
归属网络的BSF
拜访网络BSF或通用鉴权框架代理
拜访网络的BM-SC
201 执行AKA互鉴权，且用户得到了TID
202 请求拜访网络的MBMS业务，且携带了TID
204 拜访网络的BSF或通用鉴权框架代理根据TID标识信息判断用户所属的归属网络
203 查询该TID的相关信息
206 查找到TID相关的资料，并进行处理
205 查询该TID的相关信息
207 返回TID相关的资料信息
208 返回TID相关的资料信息
209 响应用户的业务请求

图 2

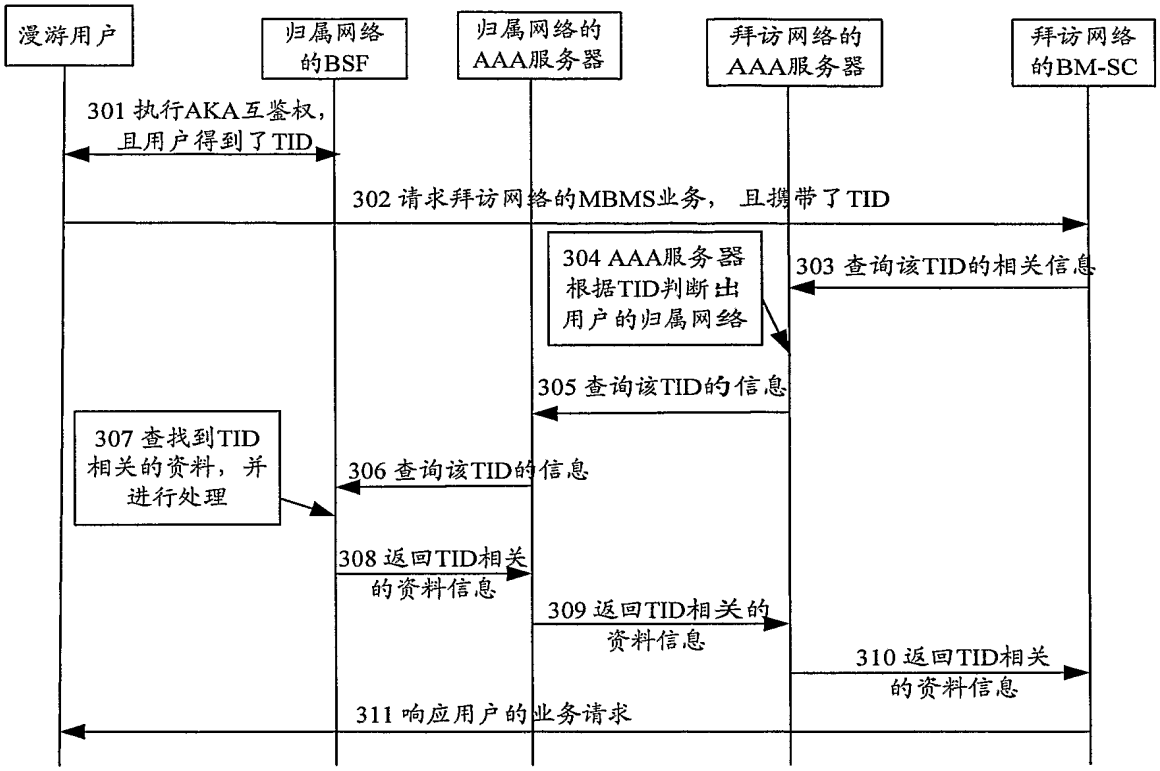

漫游用户
归属网络的BSF
归属网络的AAA服务器
拜访网络的AAA服务器
拜访网络的BM-SC
301 执行AKA互鉴权，且用户得到了TID
302 请求拜访网络的MBMS业务，且携带了TID
304 AAA服务器根据TID判断出用户的归属网络
303 查询该TID的相关信息
305 查询该TID的信息
307 查找到TID相关的资料，并进行处理
306 查询该TID的信息
308 返回TID相关的资料信息
309 返回TID相关的资料信息
310 返回TID相关的资料信息
311 响应用户的业务请求

图 3

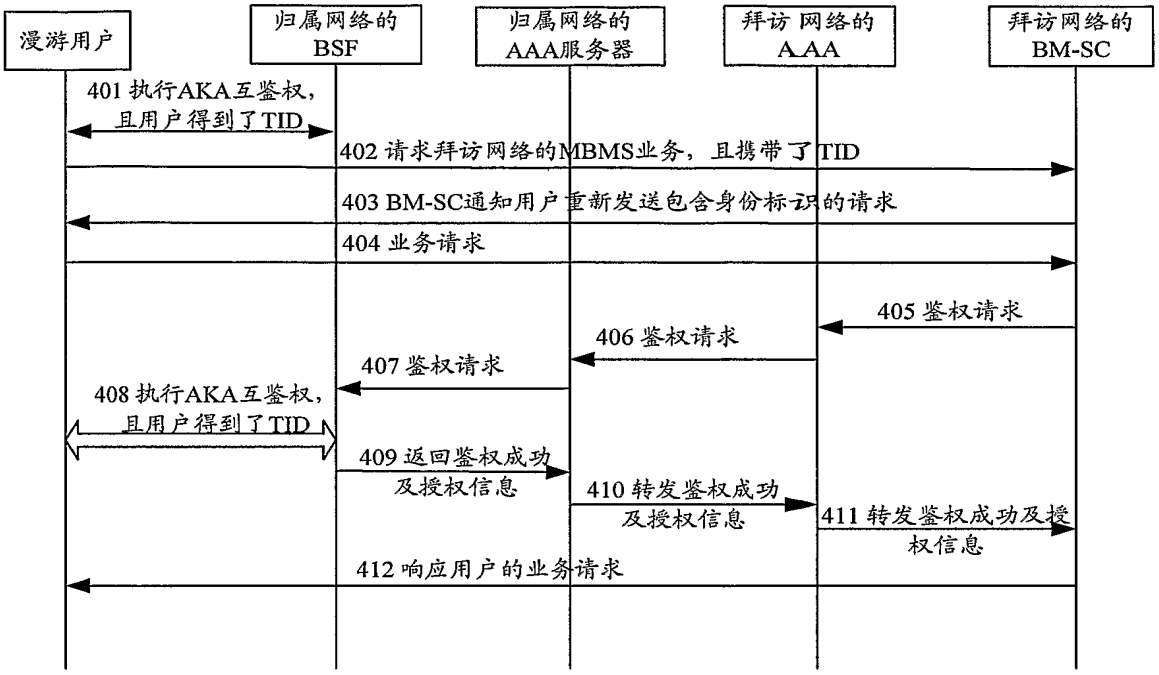

漫游用户
归属网络的BSF
归属网络的AAA服务器
拜访 网络的AAA
拜访网络的BM-SC
401 执行AKA互鉴权，且用户得到了TID
402 请求拜访网络的MBMS业务，且携带了TID
403 BM-SC通知用户重新发送包含身份标识的请求
404 业务请求
405 鉴权请求
406 鉴权请求
407 鉴权请求
408 执行AKA互鉴权，且用户得到了TID
409 返回鉴权成功及授权信息
410 转发鉴权成功及授权信息
411 转发鉴权成功及授权信息
412 响应用户的业务请求

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/000376

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]: H04Q7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: H04Q7/00 7/20 7/24 7/38 H04B7/26 H04L12/28 12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CNPAT

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI、EPODOC、PAJ: roam+ authenticat+ authorizat+ security association verification 3G HSS AAA identify checkup

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO03055237A ((MOTI) MOTOROLA INC) 03.7 月 2003 (03.07.03) See the whole document	1-9
A	US6526033B1 ((LUCE) LUCENT TECHNOLOGIES INC) 25.2 月 2003 (25.02.2003) See the whole document	1-9
A	KR2002086993A ((SKTE-N) SK TELECOM CO LTD) 21.11 月 2002 (21.11.2002) See the whole document	1-9
A	KR2003025751A ((MERC-N) MERCURY CORP) 29.3 月 2003 (29.03.2003) See the whole document	1-9
A	KR2001017852A ((KOEL-N) KOREA ELECTRONICS & TELECOM RES INST) 05.3 月 2001 (05.03.2001) See the whole document	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23.Jun 2005 (23.06.2005)	07 JUL 2005 (07.07.2005)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer Liu xinke Telephone No. (86-10)62084595

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/000376

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO03055237A	03.07.2003	WO03055237A	03.07.2003
		EP1322130A	25.06.2003
US6526033B1	25.02.2003	US6526033B1	25.02.2003
KR2002086993A	21.11.2002	KR2002086993A	21.11.2002
KR2003025751A	29.03.2003	KR2003025751A	29.03.2003
KR2001017852A	05.03.2001	KR2001017852A	05.03.2001

国际检索报告

国际申请号 PCT/CN2005/000376

A. 主题的分类

IPC[7]: H04Q7/24

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7]: H04Q7/00 7/20 7/24 7/38 H04B7/26 H04L12/28 12/66

包含在检索领域中的除最低限度文献以外的检索文献

CNPAT:漫游 拜访 鉴权 3G 安全 信任 归属

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI、EPODOC、PAJ: roam+ authenticat+ authorizat+ security association verification 3G HSS AAA identify checkup

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WO03055237A ((MOTI) MOTOROLA INC) 03.7 月 2003 (03.07.O3) 全文	1-9
A	US6526033B1 ((LUCE) LUCENT TECHNOLOGIES INC) 25.2 月 2003 (25.02.2003) 全文	1-9
A	KR2002086993A ((SKTE-N) SK TELECOM CO LTD) 21.11 月 20O2 (21.11.2002) 全文	1-9
A	KR2003025751A ((MERC-N) MERCURY CORP) 29.3 月 2003 (29.03.2003) 全文	1-9
A	KR2001017852A ((KOEL-N) KOREA ELECTRONICS & TELECOM RES INST) 05.3 月 2001 (05.03.2001) 全文	1-9

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
23.6 月 2005 (23.06.2005)	07 · 7月 2005 (07 · 07 · 2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 刘欣科 电话号码：(86-10)62084595

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/000376

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO03055237A	03.07.2003	WO03055237A	03.07.2003
		EP1322130A	25.06.2003
US6526033B1	25.02.2003	US6526033B1	25.02.2003
KR2002086993A	21.11.2002	KR2002086993A	21.11.2002
KR2003025751A	29.03.2003	KR2003025751A	29.03.2003
KR2001017852A	05.03.2001	KR2001017852A	05.03.2001